安识科技漏洞扫描

服务技术白皮书

上海安识网络科技有限公司

目录

第1章 前言

1.1. 应用频繁带病上线，传统开发模式亟需转变

目前绝大多数政企用户对业务应用漏洞的发现除了内部自测以外，多半源自外部第三方白帽子或安全厂商。漏洞爆出后，SRC 负责通知安全运维人员、项目经理、研发、测试、甚至技术负责人后才能把这个漏洞解决掉。统计显示，产品上线后，修复一个漏洞成本至少是 3 万元；而在早期，在研发过程中的，发现一个漏洞并完成修复的成本仅仅是 600 元。软件开发生命周期中，不同阶段修复安全漏洞的成本差距显著，研发测试阶段与运营阶段的修复成本甚至能够相差数百倍，因此，如何把安全漏洞消灭在萌芽状态，防止应用带病上线，是一项迫切必要的工作。

1.2. 自动化攻击成为趋势，应用漏洞风险愈发明显

伴随人工智能等新技术的应用，网络武器泄露的延续效应正在逐渐转变网络攻击的逻辑和手段，“攻防不对等”形势更为严峻。一、攻击技术越发先进智能，攻击手段在潜伏性、隐蔽性、定向性、自主性、融合性等方面能力日益增强，智能分析使得快速绕过多重防御手段成为可能。二、自动化攻击时代悄然来临，大量新兴自动化攻击工具不断涌现，令攻击门槛大幅度降低。三、网络武器研发和利用提速，基于未知漏洞的攻击利用危害不断加深，敏感数据泄露事件频频发生。

1.3. 软件开源大行其道，供应链安全保障迫在眉睫

近年来，开源软件的使用范围正在不断扩大，“拥抱开源”也成了一种企业间的普遍趋势。过于巨大的新增开源代码数量，导致单纯通过人力难以发现全部的问题，这就对漏洞挖掘、安全防范提出了更高的自动化要求。开源软件数量的增长使软件库之间的引用关系变得愈发复杂，如果其中一个环节出现了问题，就会导致所有使用该软件库的下游软件均存在该漏洞。

1.4. 业务规模日趋庞大，全面资产扫描刻不容缓

随着数字经济的快速普及，政企用户线上应用资产日趋复杂多样，不仅包含了大量被闲置的、被疏忽的“隐形”应用生产系统，甚至还有员工违规私自搭建的其他办公应用系统。由于业务频繁迭代、不定期更新等原因，一些已下线的业务资产常常被遗忘在外又无人进行管理，“非法用户”直接通过入侵这些业务即可进一步获取政企用户敏感数据。这无疑大大增加了业务资产安全管理的难度，同时也给攻击者预留了可乘之机。

对于攻击者或“非法用户”来说，目标系统的方方面面皆可能存在脆弱性，包括常见的 Web 通用漏洞、业务逻辑漏洞、服务弱口令、系统服务漏洞，也包括容易被忽略的边界资产，开放给上下游企业的 API 接口，以及由于内部员工造成的代码泄露、内部账号泄露等。而从传统检测防御的角度来看，往往只能发现一些常规的漏洞，存在许多安全盲区。

因此，政企用户需要对自身的 Web 应用业务及其关联资产进行清晰、全面的清点，持续收集与自身相关的域名、IP、主机、应用等信息，针对黑客的跳板式攻击，需全面检测关联资产，发现薄弱环节，不放过任何可能的跳板风险，确保攻击面全覆盖。

1.5. 国家政策和行业要求

《网络安全法》及新版《等级保护》中要求网络运营者应定期对自身业务进行安全测评，形成安全测评报告，并及时对发现的隐患进行修补或评估可能的影响后进行修补。

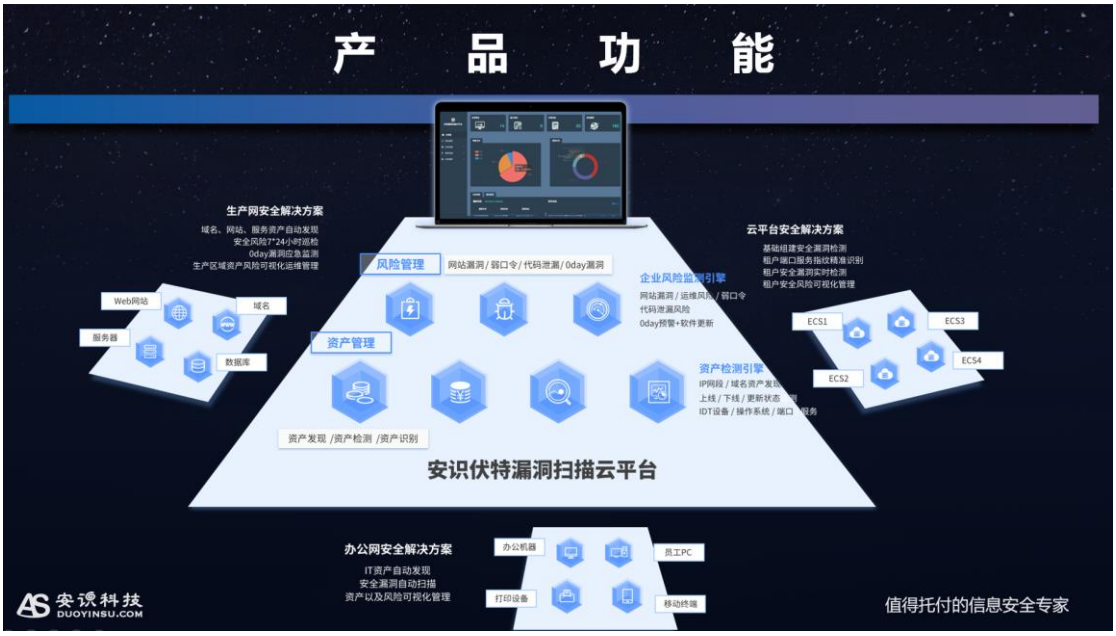
第2章 漏洞扫描服务产品介绍

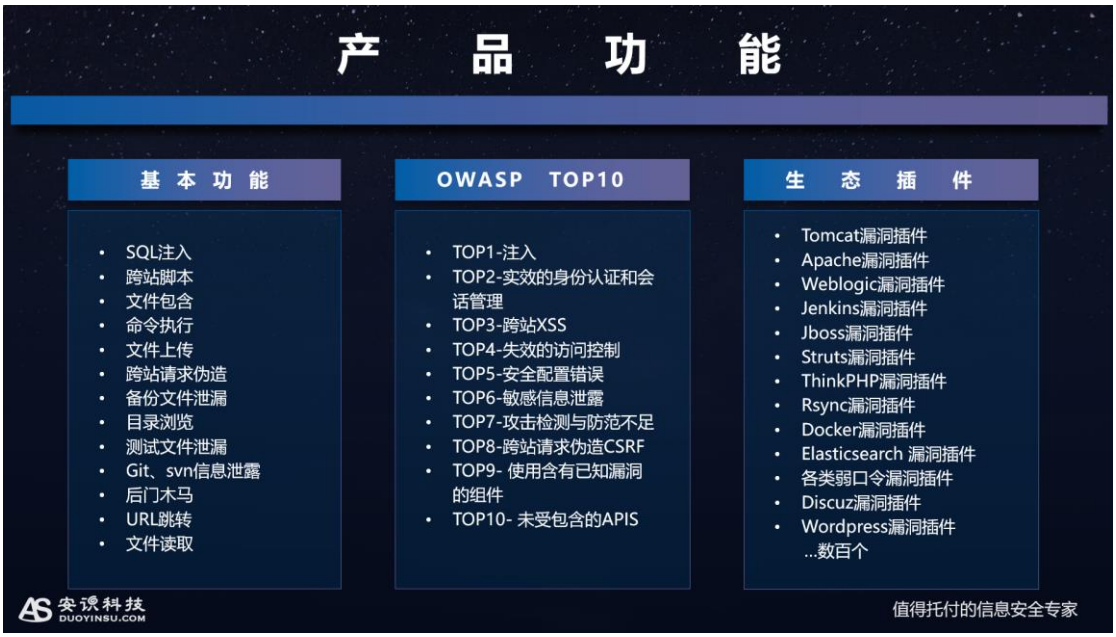
2.1. 服务产品概述

漏洞扫描，是通过自研的专业扫描产品（伏特分布式漏洞扫描云平台）对业务系统进行自动化安全漏洞检测，并由安全专家对自动化形成的漏洞扫描报复核后，交付人工报告和相关答疑服务。

伏特分布式漏洞扫描云平台，一个由社区众多安全研究人员维护的企业在线安全检测平台，企业可以在伏特对自己的企业网络进行安全漏洞检测和监控以发现潜藏在网络里的重要安全问题。

2.2. 服务产品功能





2.3. 覆盖漏洞类型

覆盖漏洞类型			
XSS	SQL 注入	敏感信息泄露	任意跳转
任意文件上传	任意文件修改	任意文件读取	任意文件下载
文件包含	水平越权	垂直越权	弱口令/未授权访问
命令注入	命令执行	CSRF	XML 实体注入
CRLF 注入	SSRF	JSONP 数据劫持	代码注入
缓冲区溢出	目录穿越	XPath 注入	模板注入
批量注册	验证码绕过	登录可撞库	LDAP 注入
MX 注入	路径泄露	源码泄露	接口暴露
SSL 风险	反序列化漏洞	特定框架、软件漏洞	竞争条件
路径遍历	接口无限制调用	设计缺陷	Cookie 注入
业务流程乱序	信息枚举泄露	账户可猜解	短信/邮箱轰炸

第3章 伏特分布式漏洞扫描云平台的优势

3.1. 丰富的漏洞知识库

漏洞知识库涵盖对各种主流操作系统、网络设备、安全设备、数据库、应用程序的漏洞检测。知识库中的漏洞信息、漏洞描述全中文展示。WEB 漏 洞知识库全面支持 OWASP TOP 10 检测，支持对当前各种主流的 WEB 应用、WEB 容器、国内外主流 CMS 及各类第三方组件的 常见漏洞检测。漏洞修复建议清晰、详细，可操作性强。漏洞知识库更新频率保持每周至少一次，重大漏洞即时更新。

3.2. 分布式部署扫描速度快

应用场景包括网络设备、虚拟平台、混合式网络、操作系统、数据库、Web 应用服务。

3.3. 扫描服务优势

使用自研爬虫程序实现全面深度的目标获取，保证扫描结果覆盖全面；众多安全研究人员编写并提交插件集成到扫描器内，由插件检测安全隐患，保证结果精度高，减少误报、漏报；提供发现网站资产和关联资产的能力，帮助企业实现资产的可视化管理；提供详细的漏洞描述和解决方案帮助企业有效理解、验证、跟踪和修复漏洞。

第4章 漏洞扫描产品服务的收益

4.1. 资产全面梳理

提供发现网站资产和关联资产的能力，结合数据大屏功能，帮助企业实现资产的可视化管理。

4.2. 安全漏洞可管理

通过漏洞扫描服务以及提供的专业详细报告，客户依据报告对发现的漏洞进行修补。